UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/505,951	02/15/2000	Simon Robert Walmsley	AUTH08US	5608

7590 01/16/2004

Kia Silverbrook
Silverbrook Research Pty Ltd
393 Darling Street
Balmain, 2041
AUSTRALIA

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	PAPER NUMBER
2137	6

DATE MAILED: 01/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

C

PRG

Office Action Summary	**Application No.** 09/505,951	**Applicant(s)** WALMSLEY ET AL.	
	Examiner Zachary A Davis	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _15 February 2000_.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-20_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-20_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _15 February 2000_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _3, 5_ .

4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: .

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sony Corporation (Kusakabe), European Patent EP 0817420, in view of Herbert et al, US Patent 6023509.

In reference to Claim 1, Sony discloses an authentication method (see Figures 7-9, Claim 1, and column 2, line 49-column 3, line 17) in which a random number is generated (column 8, lines 12-17) and encrypted with a symmetric encryption function using a first key in a first apparatus (column 9, lines 13-17). The encrypted random number is sent to a second apparatus (column 9, lines 18-21) and decrypted with a symmetric decryption function using the first key (column 9, lines 31-37), and then encrypted with the symmetric encryption function using a second key (column 9, lines 41-48) and sent to the first apparatus (column 9, line 57-column 10, line 2). The encrypted random number is compared with the originally encrypted random number (column 10, lines 29-31) after first being decrypted with the symmetric decryption function using the second key (column 10, lines 21-28). The two numbers matching authenticates the second apparatus (column 10, lines 31-35) and the two numbers not matching does not authenticate the second apparatus (column 10, lines 36-39). However, Sony does not disclose the calculation and comparison of a digital signature as a step of the authentication method.

Herbert teaches that a digital signature "authenticates or verifies that the message sent could have only originated from the signatory" (column 1, lines 31-33). A signature is calculated from and sent with a message, and the recipient of the signature computes a second version of the signature. If the received and computed signatures match, then the signature is verified (see column 1, lines 33-44). Herbert further discusses methods in which a digital signature may be computed and suggestions for improving the security in some uses of digital signatures. Additionally, Herbert discusses the use of random numbers for calculating digital signatures (column 3, lines 64-67).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as disclosed by Sony by adding the use of a digital signature for the purpose of verifying that the message (that is, the encrypted random number) could only have originated from the signatory (the first apparatus), giving increased authentication to the process (see Herbert, column 1, lines 31-44).

In reference to Claim 2, Sony and Herbert disclose everything as applied to Claim 1 above, and Sony further discloses that the first and second keys are held in both the first and second apparatuses (see Figure 9).

In reference to Claim 3, Sony and Herbert disclose everything as applied to Claim 1 above, and Sony further discloses that the first apparatus contains a random function to generate random numbers (column 8, lines 12-15). Additionally, Herbert discloses seeding a function with an initialization block (column 3, lines 22-23).

In reference to Claim 4, Sony and Herbert disclose everything as applied to Claim 1 above, and Sony further discloses that the second apparatus holds a decryption function (column 9, lines 31-37).

In reference to Claim 5, Sony and Herbert disclose everything as applied to Claim 1 above, and Herbert further discloses that with the use of the SHA-1 hashing algorithm, hashes of 160 bits can be used to create digital signatures (column 3, lines 31-34).

In reference to Claim 6, Sony and Herbert disclose everything as applied to Claim 1 above, and Sony further discloses that the second apparatus decrypts the random number with the first key (column 9, lines 31-37), encrypts the random number with the second key (column 9, lines 41-48), and sends the encrypted random number to the first apparatus (column 9, line 57-column 10, line 2). Further, Herbert, as applied to Claim 1, suggests the use of a digital signature. Specifically, the digital signature would be tested in the second apparatus, and would allow the authentication to proceed if the signature was verified, or would not authenticate the second apparatus if the signature was not verified and would end the authentication process (Herbert, column 1, lines 33-44, and see also Sony, column 10, lines 36-39).

In reference to Claim 7, Sony and Herbert disclose everything as applied to Claim 6 above, and Sony further discloses that the second apparatus monitors the time elapsed between steps of its processing (column 10, lines 53-56).

In reference to Claim 8, Sony and Herbert disclose everything as applied to Claim 1 above, and Sony further discloses that the function generating the random numbers is held in the first apparatus (column 8, lines 12-15). Additionally, Sony discloses that if the second apparatus is not authenticated, the authentication process is terminated (column 10, lines 36-39).

In reference to Claim 9, Sony and Herbert disclose everything as applied to Claim 8 above, and Sony further discloses that the first apparatus monitors the time elapsed between steps of its processing (column 10, lines 6-7).

In reference to Claim 10, Sony and Herbert disclose everything as applied to Claim 1 above, and Sony further discloses that it is determined if the second apparatus is valid (column 10, lines 31-35) or not (column 10, lines 36-39).

Claims 11-20 are system claims corresponding substantially to the method steps of Claims 1-10, and are thus rejected by a similar rationale.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A Davis whose telephone number is (703) 305-8902. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

zad

Matthew D. Smithers
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137